Anemone Technology
-we make your technology bloom

Critical paths to C-ITS deployment

Niels Peter Skov Andersen
Anemone Technology

- Freezing HW and SW requirements
- Spectrum
- Security
- Privacy
- Compliance Assessment

- Freezing HW and SW requirements
- Spectrum
- Security
- Privacy
- Compliance Assessment

Freezing the Hardware Requirements

Need for a stable base for the Hardware design – This includes

- RF parameters
- Data storage requirements
  - Database definition for Tolling
  - Decision on potential revocation list and their size etc.
  - Pseudonym policy
- Protection profile for V2X module
- Technical solution for crypto agility for day 1 units
- Privacy requirements – what will be the impact on implementation
- Test specifications – Test requirements

Freezing the Software Requirements

Need for a stable base for the software design – This includes amongst others

- Data storage requirements
  - Database definition for Tolling
  - Decision on potential revocation list and their size etc.
  - Pseudonym policy
- Protection profile for V2X module
- Technical solution for crypto agility for day 1 units
- Privacy requirements – Will there special requirements for signaling consent etc.
- Test specifications

Status

- Technology is ready for deployment of the first applications
- Parts of framework for deployment is still under development for allowing a common European deployment
  - Regulatory
  - Policy
- Key focus areas to enable deployment
  - Spectrum
  - Compliance Assessment
  - Security
  - Privacy

- Freezing HW and SW requirements
- Spectrum
- Security
- Privacy
- Compliance Assessment

Spectrum issues

- Key is the Harmonized Standard EN 302 571
  - Sent for public enquiry 2Q2016
  - Comments resolved during 3Q2016
  - Sent for final vote 4Q2016
  - Positive vote received on 6 February 2017
  - Awaiting publication in the OJEU
- Reflects updated spectrum regulation DEC(08)01 and REC(08)01
- Mitigation towards Tolling (DSRC) has been resolved

- Freezing HW and SW requirements
- Spectrum
- Security
- Privacy
- Compliance Assessment

Security

- Stable first draft of a Common European Certification Policy
  - Support both NIST and Brainpool – max key length on the radio (ETSI G5) 256
- Common European Security Policy still in its infancy
- Establishment of common PKI framework
  - Agreement on model allowing multiple Root CAs, but keeping a single point of contact and having a common governance structure
  - Still open who will setup the infrastructure
  - Initial and long term financing still open

- Freezing HW and SW requirements
- Spectrum
- Security
- Privacy
- Compliance Assessment

Privacy

- CAM and DENM considered personal data
- Current privacy legislation is based on a one to one relation between known parties not on a broadcast scenario - one to many not necessarily identified parties
- Work in progress to describe the system and the mitigations measures that are a part of the C-ITS from a privacy point of view
- Current expectation is to have feedback in July 2017 from the Article 29 Working Party
  - Are additional measures required ?
  - What lvel of impact will such measure have on current implementations ?

- Freezing HW and SW requirements
- Spectrum
- Security
- Privacy
- Compliance Assessment

Compliance Assessment

- Test specifications exist from ETSI, C2C-CC and pilot projects exist
- Successful large scale interoperability organized by ETSI in November 2016 in Livorno, Italy. But formal compliance assessment is different to interoperability testing.
- However, formal compliance assessment framework still not established
  - What is the scope of the compliance assessment
  - Who sets and what are the compliance assessment criteria
  - How to verify the test cases
  - Who will perform the test
- Interim compliance assessment regime might be needed

Questions ?

Further information

codecs-project.eu

cimec-project.eu

car-2-car.org

amsterdamgroup.mett.nl